



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/493,984	01/28/2000	Robert S. Eisenbart	18926-003220US	2907

20350 7590 02/17/2006

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER

SIMITOSKI, MICHAEL J

ART UNIT PAPER NUMBER

2134

DATE MAILED: 02/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/493,984

Applicant(s)

EISENBART ET AL.

Examiner

Michael J. Simitoski

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 December 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,2,4-19 and 21-23 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,2,4-19 and 21-23 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 13 July 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The response of 12/7/2005 was received and considered.
2. Claims 1-2, 4-19 & 21-23 are pending.

Response to Arguments

3. Applicant's arguments with respect to claims 1-2, 4-19 & 21-23 have been considered but are moot in view of the new ground(s) of rejection. However, the Wasilewski reference will be discussed.
4. In light of Applicant's amendments to the claims, the rejections based on the cited art to Gennaro and Wong are withdrawn.
5. Applicant's response (p. 9) argues that Wasilewski does not disclose generating a signatory group comprising at least a portion of a first information and at least a portion of a second information and generating a signature over the signatory group. However, Wasilewski discloses concatenating a clear control word/second information and an MSK/first information to produce a concatenation/signatory group (col. 9, lines 31-35). The concatenation/signatory group is then hashed/signed (col. 9, lines 35-38). The signature/MAC is appended to the control word/second information and sent to the set top box (col. 9, lines 41-46). The MSK/first information is transmitted separately (col. 9, lines 50-52).

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-2, 4-6, 8-9, 11-13 & 21 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 5,870,474 to Wasilewski et al. (**Wasilewski**).

Regarding claims 1, 8 & 11, Wasilewski discloses generating a signatory group comprising at least a portion of a first information/MSK and at least a portion of a second information/clear code word (col. 9, lines 31-46), generating a signature over the signatory group (col. 9, lines 31-46), appending the signature/hash to one of the first information or the second information (appended to second information/clear code word) (col. 9, lines 40-46), sending the first information/MSK over a network (col. 11, lines 4-48), sending the second information/clear code word over the network separately from the step of sending the first information (col. 9, lines 40-46) and sending the signature over the network separately from at least one of the first information or the second information (separate from the first information/MSK) (col. 9, lines 31-46 & col. 11, lines 4-48).

Regarding claims 2 & 9, Wasilewski discloses the first information/MSK comprising an authorization data structure/key (col. 9, lines 47-52) and the second information/clear code word comprising a software object/key (col. 9, lines 30-46).

Regarding claim 4, Wasilewski discloses determining which resources a software object in the second information/clear code word is entitled to interact with (which blocks of packets they can decrypt) (col. 8, lines 48-60).

Regarding claim 5, Wasilewski lacks explicitly waiting a predetermined time period after the step of sending the first information before sending the second information. However, it is inherent that, in a packet-based network, a predetermined time period (transmission rate) is waited between each packet, and hence between each piece of information.

Regarding claim 6, Wasilewski discloses the first information/MSK including authorization information for an associated software object/clear code word (col. 9, lines 30-35).

Regarding claim 12, Wasilewski discloses determining a lifetime for which the second information is usable (col. 8, lines 48-60).

Regarding claim 13, Wasilewski discloses checking the first information/MSK for an authorization corresponding to the second information/clear code word (decrypting) (col. 8, lines 25-28).

Regarding claim 21, Wasilewski discloses determining if access of at least one of the first or second information is authorized (determining if control word is authorized) (col. 9, lines 47-58) and ignoring the second information/control word if not authorized (col. 9, lines 47-58).

8. Claims 7, 10, 14-15 & 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Wasilewski**, as applied to claims 1 and 8 above, in view of U.S. Patent 5,247,364 to Banker et al. (**Banker**).

Regarding claims 7 & 10, Wasilewski discloses a system, but lacks sending information over different transmission pathways. Banker teaches that unlike in-band transactions, out-of-band subscriber terminals receive data over this channel no matter what the channel the subscriber is tuned to (col. 1, lines 28-44 & col. 2, lines 55-68). Therefore, it would have been

Art Unit: 2134

obvious to one having ordinary skill in the art at the time the invention was made to include the first information on a different transmission pathway than the second information. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of delivery regardless of which channel a subscriber was tuned to, as taught by Banker (col. 1, lines 28-44 & col. 2, lines 55-68).

Regarding claim 14, Wasilewski discloses an information object/MSK, authorization information/clear code word wherein a signature/hash is generated over the information object/MSK and the authorization information/clear code word (col. 9, lines 30-38), wherein the signature/hash is integral to one of the information object or the authorization information (integral with the authorization information/ clear code word) (col. 9, lines 40-46). Wasilewski lacks the information object using a first transmission pathway to a set top box, the authorization information using a second transmission pathway to the set top box that is different from the first transmission pathway and the signature using a third transmission pathway to the set top box that is different from at least one of the first or second transmission pathways. However, Banker teaches that unlike in-band transactions, out-of-band subscriber terminals receive data over this channel no matter what the channel the subscriber is tuned to (col. 1, lines 28-44 & col. 2, lines 55-68). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include the first information on a different transmission pathway than the second information. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of delivery regardless of which channel a subscriber was tuned to, as taught by Banker (col. 1, lines 28-44 & col. 2, lines 55-68).

Regarding claim 15, Wasilewski discloses an authorization message/ECM, which includes the authorization information/clear code word and the signature (col. 9, lines 40-46).

Regarding claim 19, Wasilewski discloses the information object/MSK sent separately over a network from the authorization information/clear code word (col. 11, lines 10-15).

9. Claims 16 & 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Wasilewski** in view of **Banker**, as applied to claim 14 above, in further in view of U.S. Patent 6,157,721 to Shear et al. (**Shear**). Wasilewski discloses a system, as modified above, that uses digital signatures for verification, but is silent regarding multiple signatures. Shear teaches that using several dissimilar digital signatures, via different algorithms, can reduce vulnerability from algorithm compromise (ABSTRACT & col. 7, lines 9-18). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a plurality of signatures with different signing algorithms in Banker's data and to use one or more of the signatures to validate the data. One of ordinary skill in the art would have been motivated to perform such a modification to reduce vulnerability from algorithm compromise, as taught by Shear (ABSTRACT & col. 7, lines 9-18).

10. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Wasilewski** in view of **Banker**, as applied to claim 14 above, in further in view of U.S. Patent 5,420,866 to Wasilewski (**Wasilewski '866**). Wasilewski, as modified above, is silent regarding including tiers in the authorization information. However, Wasilewski '866 teaches that satellite and cable access providers include tier information with authorization information sent to decoders to

control access to different tiers of programs (col. 4, lines 51-59). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include tier information in the authorization information. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of controlling access to different tiers of programs in a television subscription service, as taught by Wasilewski '866 (col. 4, lines 51-59).

11. Claims 22 & 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Wasilewski**, as applied to claims 1 and 8 above, in view of **Shear**. Wasilewski discloses a system that uses digital signatures for verification, but is silent regarding multiple signatures. Shear teaches that using several dissimilar digital signatures, via different algorithms, can reduce vulnerability from algorithm compromise (ABSTRACT & col. 7, lines 9-18). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a plurality of signatures with different signing algorithms in Banker's data and to use one or more of the signatures to validate the data. One of ordinary skill in the art would have been motivated to perform such a modification to reduce vulnerability from algorithm compromise, as taught by Shear (ABSTRACT & col. 7, lines 9-18).

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841.

The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. - 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Or faxed to:

(571) 273-8300
(for formal communications intended for entry)

Or:

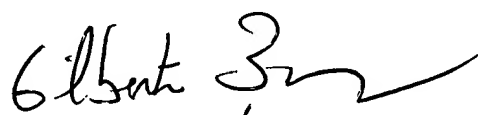
(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



MJS
February 13, 2006



GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100